Michael D. Adams

30 June 2013

Re: Proceeding RM-11699

This is an extension to my previously-submitted comments, and a response to various comments submitted as regards RM-11699. Please note that the opinions expressed in this submission are mine alone; they are not necessarily those of employers past or present, or organizations I am currently or formerly a member of.

First, I wish to restate my opinion that I cautiously support the idea of permitting the use of encryption in the amateur radio service in very limited circumstances.

Various commenters have raised several points in objecting to the proposed rulemaking which, while valid concerns, I believe do not necessitate the rejection of the proposal.

Applicability of HIPAA / other regulations

Several commenters have correctly noted that HIPAA does not, of itself, require encryption of information, and that exceptions can be made in case of emergency. While that is probably correct, it is perhaps myopic to focus on only the text of HIPAA.

For one thing, a challenge faced by volunteer communicators is not the body of HIPAA itself, but in certain served agencies' reactions to HIPAA and similar regulations. In this day where identity theft is common, where some citizens have become aware of the implications of the sharing of their personal information, and where society in general has become ridiculously litigious, is it any wonder that agencies that potentially might make use of volunteers from the amateur radio service are overly conservative on the subject?

Also, while much has been made about the (in)applicability of HIPAA, it should be noted that HIPAA is not the sole federal or state legislation or regulation governing the protection of personal information. For example, the Commission should be aware of Massachusetts' stringent privacy regulations, in particular 201 CMR 17.04:

> Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:[…]

> (3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and **encryption of all data containing personal information to be transmitted wirelessly.** [emphasis added]

MARS

A few commenters have noted that encryption for volunteer communicators is already available through the Military Auxiliary Radio System (MARS). As a member of Navy MARS myself, I agree that this is one consideration that helps sell the usefulness of MARS in discussions about the role of volunteer communicators in disaster preparation.

However, I believe the "MARS has encryption; the amateur radio service therefore does not need it" argument fails on two grounds:

First, the charters of the three MARS programs currently extends only to the support of federal, state, or local government entities. To the best of my knowledge, MARS is not currently authorized to directly support hospitals or non-governmental response agencies, both of which may be more likely to handle sensitive personal information, and which are generally not protected by federal or state statutory immunities.

Second, the primary value that the amateur radio service provides in the discussion of emergency response is that hams are everywhere.[1] While many amateurs interested in emergency preparedness and public service are also members of MARS, there are still significantly fewer active MARS members (particularly those authorized to handle encrypted traffic) than hams. Assuming that the "when all else fails" path for secure communications of personal data is MARS may be so limiting as to be a nonviable concept.

Is there an actual need?

Several commenters have expressed a belief that there is not a general need for any form encryption in the amateur radio service. I agree with the notion that the situations where hams would get involved in emergency communications are those where sensitive information could be routed through surviving non-amateur circuits, or held until non-amateur communications can be reestablished. I also agree with (and applaud) the notion that other forms of messages that volunteers could be asked to pass can be constructed in ways that do not generally require the exposure of sensitive information.

[1] …or at least everywhere in those communities not dominated by properties under deed restrictions which discourage or preclude amateur radio activity.

However, I wonder if the perceived lack of need is also an artifact of encryption currently being unavailable in the amateur radio service. Do we see “no need” because we have simply never considered the possibilities?

Isn’t that one aspect of amateur radio – providing the opportunity for non-professional communicators and enthusiasts to “explore the possibilities” as regards to wireless communication?

In addition, as noted above, part of the challenge amateur radio is facing as our information society matures and technology advances, is not whether there is an actual need; it’s whether there is a perceived need by agencies potentially seeking assistance from amateurs? If an NGO’s lawyer tells the NGO to not bother with hams as volunteers because of our inability to provide a means to protect sensitive information, does it matter whether there are workarounds that do not require encryption?

Impact on self-policing nature of the amateur radio service

Multiple commenters have noted the potential for any expansion of encryption in the amateur radio service to damage the self-policing nature of the service.

I think this is a valid, but not unresolvable concern.

It should be noted that the petition is seeking only a limited expansion of encryption, authorizing handling encrypted third-party traffic domestically during emergencies, and for related training. I do not believe that authorizing encryption under such circumstances would damage the essential nature of amateur radio, but there may be revisions to the petitioner’s proposal that could be made to address the concerns expressed by multiple commenters. Specifically:

1. Clarify that encryption is authorized for handling third-party traffic within the United States only in emergencies where conventional communications channels are inoperative or significantly impaired, and that this exception for emergencies does not extend to first party traffic.

2. As regards the training exception:

    a. Limit training exercises which involve transmission or reception of signals on HF to no more than 3 hours in any 90 day period for any station.[2]

    b. Require that in such training exercises, any encrypted message be accompanied by an unencrypted version of the message, an announcement of the mode of encryption,

[2] Given the local nature of VHF and higher bands, such frequencies may be more suitable for any additional experimentation required beyond the fairly stringent 3 hours/90 days guideline I suggest.

and either a copy of the key or cipher or an announcement of where the key/cipher can be obtained. This additional information should be provided in the same mode and at the same speed as the encrypted message.

3. Reiterate that station identification shall be made without encryption or cipher.

4. Require appropriate logging, retention of logs, and retention of copies of all training exercise traffic for possible inspection.

Modes of Encryption, Key Handling; Experimentation

Several commenters have expressed concerns or offered ideas regarding how encryption can be achieved, and regarding the challenges of handling encryption keys.

Many of these comments have been quite interesting, in my opinion, but I believe that prescription of best practices as regards to tools and protocols are likely beyond the scope of Part 97.

One of the *raisons d'être* of the amateur radio service is to provide a sandbox for nonprofessionals to experiment with the art and science of wireless communication. However, no one can deny modern wireless non-amateur communication increasingly involves new modes and data obfuscation techniques, accompanying the evolution of our information based society.

The opportunity to explore the use of encryption, including message formatting and key handling, is something that is currently lacking in the sandbox aspect of the amateur radio service. Given the tradition of open communication, and international regulations generally governing amateur radio, it would be inappropriate to allow such experimentation willy-nilly. However, this proposal presents the Commission an opportunity to authorize amateurs to explore such techniques in a measured, limited manner.

I thank the Commission again for the opportunity to comment on this manner. I hope that you will grant the petitioner's proposal, perhaps with the revisions discussed above.

Sincerely,

Michael D. Adams